SOC IMS: SWI-20110808-224136

Last Updated: 7/21/2016 8:04 PM

SOC Incident Management System

IMS User Contact:	(b) (6), (b)	**Restrict Access To:**	All IMS
Record Permissions Group:	All IMS Users	**Record Source:**	

Contact Details

Enter the NASA AUID or email address of the Contact, and click "Lookup Contact Details" to automatically retrieve the information.

AUID:		**Email:**	

Enter Contact information below if the primary contact is not an IMS user

Contact Last Name:	(b) (6)	**Contact First Name:**	(b) (6), (b) (7)
Contact Role:	Other	**Contact Office Phone:**	(b) (6), (b)
Contact E-mail:	(b) (6), (b) (7)(C)	**Contact Cell Phone:**	
Contact AUID:		**Contact NASA Center:**	
Contact Building:		**Contact Room Number:**	
Contact Type:			

General Details

SOC Tracking Number:	SWI-20110808-224136	**Categorization:**	Work-Item
Date Record Created (UTC):	8/8/2011 2:54 PM	**Incident Time Zone:**	UTC - Coordinated Universal Time Zone (GMT)
Title:	NASA user password and more		
Brief Description:	Looks like Teampoison and Anonymous are releasing something with regards to this. Their MO is usually SQLi, and dump any and everything they can. So can probably pivot around any publicly facing web systems that the user in this dump has access to and watch flow (historically.) (b) (7)(E) Also contains hashed pw which is likely crackable.		
Current Status:	Closed	**Assigned To:**	SOC Tier-2
Current Priority:	Medium	**Also Notify:**	
CUI:	Maybe SBU Only	**Notify on Save:**	No

CUI Categories:	
Ok To Close:	No

Sensitive But Unclassified

Reason SBU is suspected to be involved:		**How SBU was disclosed:**	
SBU Media Format:		**SBU Media Format Medium:**	
Date & Time Incident Occurred:		**Date & Time of Discovery of SBU Loss:**	
Scope of SBU Exposure:		**SBU Data Elements Exposed:**	
Original Information Owner:		**Number of Individuals without the appropriate "Need to Know" for Information Associated with this Exposure:**	
Protection of SBU Data Elements:		**SBU Trade Secrets:**	
Law Enforcement or IG Notified about SBU:		**Time to Report:**	

Work Item Due Date

Due Date:		**Due Date (UTC):**	

Related Tasks

Task ID	Assigned To	Due Date (UTC)	Priority	Status	Description	Resolution
224176	ARC IRM ARC IRT ARC ITSM	8/8/2011 5:43 PM	High	Complete	NASA user (b) (6), (b) (7)(C) has their password hash listed possibly by anonymous another hacker group. This may be all the info they have, but it may also be an indication of an upcoming release of data for	hash is from the vbulletin install on (b) (7)(E) (see SOC-20110808-224190). This is the only place this password is used and the system has been taken offline for console review.

Related Incidents

Select Relationship:		Relationship Description:	

Parent Incident

SOC Tracking Number	Current Status	Title
No Records Found		

Child Incidents

SOC Tracking Number	Current Status	Title
No Records Found		

Sibling Incidents

SOC Tracking Number	Current Status	Title
No Records Found		

Lost or Stolen NASA Equipment Application

Tracking ID	Cause of Loss	Type of System Lost	Description of Circumstances
No Records Found			

Host Information

NASA Hosts

IP Address	IPv6 Address	Host Name	Center/Facility
No Records Found			

External Hosts

IP Address	External IPv6 Address	Host Name	Position in this attack
No Records Found			

Campaigns

Campaign Name:		Reviewed By TVA:	

Campaign Comment:		**Confirmed By TVA:**	
		Is APT:	

Indicators of Compromise

IOC Domain

FQDN	Do Sinkhole	Comment
No Records Found		

IOC IP

IP Address	IP Block	Comment
No Records Found		

IOC File

Filename	MD5 Hash	Comment
No Records Found		

IOC Registry Key

Key Name	Key Value	Comment
No Records Found		

IOC Email

Sender Email	Subject	Comment
No Records Found		

IOC Detection

Name	Type	Comment
No Records Found		

Costs

Center (Hours):		**Center (Dollars):**	
NASA SOC (Hours):		**NASA SOC (Dollars):**	
NASA NOC (Hours):		**NASA NOC (Dollars):**	
Other Costs (Hours):		**Other Costs (Dollars):**	

Total Costs in Hours and Dollars are automatically calculated as the sum of the individual costs above. Center IR teams or managers should enter the Center costs, the NASA SOC Manager should enter the SOC Costs and the NOC Manager should enter the NOC costs, if any, in order to arrive at the Total Cost.

Total Cost (Hours):		**Total Cost (Dollars):**	
Description of			

System Down Time (Days):		**System Down Time (Hours):**	

Timeline

Date Record Opened (UTC):	8/8/2011 2:54 PM	**Date Record Confirmed (UTC):**	8/11/2011 9:25 PM
Date Record Contained (UTC):	8/11/2011 9:25 PM	**Date Record Resolved (UTC):**	8/11/2011 9:25 PM
Date Record Closed (UTC):	7/21/2016 8:04 PM		
Time in Open:	3.25		
Time in Confirmed:	1805.94	**Time to Confirm:**	3.00
Time in Contained:	1805.94	**Time to Contain:**	3.27
Time in Resolved:	1805.94375	**Time to Resolve:**	3.27
Time in Closed:	858.46	**Time to Close:**	1809.22
Number of Days to Resolve:	3.272		

Journal Entries

Entry	Entry Date	IMS User
All tasks complete, closing out ticket.	8/11/2011 9:24 PM	(b) (7)(C), (b) (6)
User emailing soc@nasa.gov to report possible incident. Looked up in IMS and found this work-item. -------- Original Message -------- Subject: SQL vulner for nasa.gov Date: Mon, 8 Aug 2011 15:44:28 -0400 From: (b) (7)(C), To: soc@nasa.gov https://twitter.com/#!/TeaMp0isoN_ Posted this (b) (7)(E) As per his twitter. He is liek Anonymous and hacks sites regularly. I try to warn people when i see they are targeted. Hate these guys. I will be glad when FBI or whoever gets them all.	8/8/2011 8:14 PM	(b) (7)(C),

Admin reported a compromise of (b) (7)(E) vbulletin server. Determined the hash was found from this compromise. Tracking via SOC-20110808-224190	8/8/2011 7:45 PM	(b) (7)
Attached a screenshot sent in from (b) (7)(C), . The screenshot doesn't show the server that they're saying is compromised, but it's likely that it's related to this specific incident. Contents of his email: Also saw this one: (b) (7)(E) Perhaps the SOC can open a separate ticket to look into this one. I am not sure if the site is considered hostile or not. I've attached the image that shows the issue to this e-mail. Can't tell the site or users though.. (b)	8/8/2011 6:50 PM	(b) (7)(C),
Also on the one (b) (6), (b) were reporting (that NIH sent us earlier too): The hash itself appears to have been reported/requested for cracking on Jully 22 by user "666": (b) (7)(E) 666 Joined: 08 Feb 2011 Posts: 72 (b) (7)(E) Posted: Fri Jul 22, 2011 11:17 am Post subject: (b) (7)(E) thnx Admin (b) (7)(E)	8/8/2011 6:44 PM	(b) (7)(C),

--(b) (6), (b) IT Security Specialist NASA Office of the CIO Cyber Threat Analysis Program (CTAP) (b) (6), (b) (7)(C) On 8/8/11 1:18 PM, (b) (6), (b) " wrote:
> >
> > Also saw this one:
> >
> > (b) (7)(E)
> >
> >
> > Perhaps the SOC can open a separate ticket to look into this one. I am not
> > sure if the site is considered hostile or not. I've attached the image that
> > shows the issue to this e-mail. Can't tell the site or users though..
> >
> > (b)
> >
> >
> >
> > On 8/8/11 1:11 PM, (b) (6), (b) (HQ-WIM51)"
> > wrote:
> >
>> >> FYI, (b) (7)(E)
>> >>
>> >> ================
>> >>
>> >> Nasa Vulnerable to a public SQLi Exploit - Embarassing much?
>> >>
>> >> Admin Username (b)
>> >> Email: (b) (6), (b) (7)(C)
>> >> Hashed Password (b) (7)(E)
>> >> (b) (7)(E)
>> >>
>> >> Admin Username: (b) (6),
>> >> Email: (b) (6), (b) (7)(C)
>> >> Hashed Password (b) (7)(E)
>> >> (b) (7)(E)
>> >>
>> >> - If shit like this is vulnerable to public exploits, imagine whats
>> >> vulnerable
>> >> to private 0days :) -
>> >>
>> >> [+] TriCk - TeaMp0isoN
>> >> [+] Shoutouts: iN^SaNe - Hex00010 - MLT
>> >>
>> >> Twitter:
>> >> @TeaMp0isoN_
>> >>
>> >> **NOTE: A joint #TeaMp0isoN & #Anonymous Operation is about to hit the
>> >> interwebs soon **
>> >>
>> >> =============
>> >>
>> >> SOC folks, can you check into this to try to determine what server might have

Called (b) (6), office and cell numbers and left messages about the task for the ARC user.	8/8/2011 6:23 PM	(b) (6),
Copy/paste from (b) (7) : ========== Nasa Vulnerable to a public SQLi Exploit - Embarassing much? Admin Username: (b) Email: (b) (6), (b) (7)(C) Hashed Password (b) (7)(E) (b) (7)(E) Admin Username: (b) (6), (b) (7) Hashed Password (b) (7)(E) (b) (7)(E) - If shit like this is vulnerable to public exploits, imagine whats vulnerable to private 0days :) - [+] TriCk - TeaMp0isoN [+] Shoutouts: iN^SaNe - Hex00010 - MLT Twitter: @TeaMp0isoN_ **NOTE: A joint #TeaMp0isoN & #Anonymous Operation is about to hit the interwebs soon ** ==========	8/8/2011 5:46 PM	(b) (6),
-------- Original Message -------- Subject: NASA user password and more Date: Mon, 8 Aug 2011 10:41:42 -0400 From: (b) (6), (b) (7)(C) [C] To: 'soc@nasa.gov' Looks like Teampoison and Anonymous are releasing something with regards to this. Their MO is usually SQLi, and dump any and everything they can. So can probably pivot around any publicly facing web systems that the user in this dump has access to and watch flow (historically.) (b) (7)(E) Also contains hashed pw which is likely crackable. (b) (6), (b) (7)(C) NIH Incident Response Team (IRT) Office of the Chief Information Officer (OCIO)	8/8/2011 2:54 PM	(b) (6), (b)

National Institutes of Health, HHS
Phone: (b) (6), (b)
Fax: (301) 594-3061

E-mail (b) (6), (b) (7)(C)

IRTLogo Protecting & Supporting NIH Research

Attachment(s)

Name	Size	Type	Upload Date	Downloads
nasa.png	85727	.png	8/8/2011 6:50 PM	0

History Log

View History Log